



UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/619,176	07/15/2003	Max Hamberg	089229.00141	4987
32294 7590 08/16/2007 SQUIRE, SANDERS & DEMPSEY L.L.P. 14TH FLOOR 8000 TOWERS CRESCENT TYSONS CORNER, VA 22182			EXAMINER NGUYEN, MINH DIEU T	
			ART UNIT 2137	PAPER NUMBER
			MAIL DATE 08/16/2007	DELIVERY MODE PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Office Action Summary**Application No.**

10/619,176

Applicant(s)

HAMBERG ET AL.

Examiner

Minh Dieu Nguyen

Art Unit

2137

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --**Period for Reply**

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

- 1) ☒ Responsive to communication(s) filed on 06/04/07.
- 2a) ☒ This action is **FINAL**. 2b) ☐ This action is non-final.
- 3) ☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

- 4) ☒ Claim(s) 1-56 is/are pending in the application.
- 4a) Of the above claim(s) _____ is/are withdrawn from consideration.
- 5) ☐ Claim(s) _____ is/are allowed.
- 6) ☒ Claim(s) 1-56 is/are rejected.
- 7) ☐ Claim(s) _____ is/are objected to.
- 8) ☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

- 9) ☐ The specification is objected to by the Examiner.
- 10) ☐ The drawing(s) filed on _____ is/are: a) ☐ accepted or b) ☐ objected to by the Examiner.
Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).
Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).
- 11) ☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

- 12) ☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
- a) ☐ All b) ☐ Some * c) ☐ None of:
1. ☐ Certified copies of the priority documents have been received.
 2. ☐ Certified copies of the priority documents have been received in Application No. _____.
 3. ☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

- | | |
|--|---|
| 1) <input checked="" type="checkbox"/> Notice of References Cited (PTO-892) | 4) <input type="checkbox"/> Interview Summary (PTO-413) |
| 2) <input type="checkbox"/> Notice of Draftsperson's Patent Drawing Review (PTO-948) | Paper No(s)/Mail Date. _____ |
| 3) <input type="checkbox"/> Information Disclosure Statement(s) (PTO/SB/08) | 5) <input type="checkbox"/> Notice of Informal Patent Application |
| Paper No(s)/Mail Date _____ | 6) <input type="checkbox"/> Other: _____ |

DETAILED ACTION

Response to Amendment

1. This office action is in response to the communication dated 6/4/07 with the amendments to claims 1-54 and the addition of claims 55-56.
2. Claims 1-56 are pending.

Response to Arguments

3. Applicant's arguments with respect to claims 1-54 have been considered but are moot in view of the new ground(s) of rejection.

Claim Rejections - 35 USC § 102

4. The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

A person shall be entitled to a patent unless –

(e) the invention was described in (1) an application for patent, published under section 122(b), by another filed in the United States before the invention by the applicant for patent or (2) a patent granted on an application for patent by another filed in the United States before the invention by the applicant for patent, except that an international application filed under the treaty defined in section 351(a) shall have the effects for purposes of this subsection of an application filed in the United States only if the international application designated the United States and was published under Article 21(2) of such treaty in the English language.

5. Claims 1-2, 4-5, 27, 34-35, 43, 49, 51 and 55-56 are rejected under 35 U.S.C. 102(e) as anticipated by or, in the alternative, under 35 U.S.C. 103(a) as obvious over Bolosky et al. (7,043,637).

a) As to claim 1, Bolosky discloses a method comprising steps of generating a second set of data (e.g. hash value) representative of a first set of data (i.e. data file, Bolosky: col. 5, lines 39-42). A hash function is known in the art as a reproducible method of turning some kind of data into a (relatively) small number that may serve as a digital representative of the data. Bolosky also discloses encrypting the first set of data using the second set of data (i.e. encrypting the file using the hash value as the key, Bolosky: col. 5, lines 42-44).

b) As to claim 2, Bolosky discloses the method of claim 1, wherein the encrypting the first set of data comprises performing a symmetric key based encryption algorithm (i.e. the same key is used for encryption and decryption, a symmetric cipher) between the first set of data and the second set of data (Bolosky: col. 5, lines 42-43).

c) As to claim 4, Bolosky discloses the method of claim 1, wherein the encrypting the first set of data comprises encrypting digital data (i.e. data file, Bolosky: col. 3, lines 32-37).

d) As to claim 5, Bolosky discloses the method of claim 1, wherein the generating the second set of data comprises generating a reduced version of the first set of data (i.e. hash value is the reduced version, Bolosky: col. 5, lines 39-42).

e) As to claim 27, Bolosky discloses the method of claim 1, wherein the encrypting the first set of data comprises encrypting one of a digital photograph, a picture or a text document, an audio file or multimedia message (i.e. data file, Bolosky: col. 3, lines 32-37).

f) As to claim 34, this claim is directed to a system implementation of the method of claim 1, therefore it is rejected by a similar rationale applied against claim 1 above.

g) As to claim 35, this claim is directed to a system implementation of the method of claim 2, therefore it is rejected by a similar rationale applied against claim 2 above.

h) As to claim 43, Bolosky discloses the system of claim 34, further comprising decrypting means for decrypting the encrypted first set of data using the second set of data (i.e. using the second set of data as a symmetric key, therefore the same key is used for both encryption and decryption, Bolosky: col. 5, lines 42-44).

i) As to claim 49, Bolosky discloses the system of claim 34, wherein the first set of data comprises one of a digital photograph, a picture or a text document, an audio file or multimedia message (i.e. data file, Bolosky: col. 3, lines 32-37).

j) As to claim 51, Bolosky discloses the system of claim 34, wherein the system comprises a single entity (Bolosky: Fig. 3).

k) As to claim 55, this claim is similar to claim 34 and is rejected by a similar rationale applied against claim 34.

l) As to claim 56, Bolosky discloses a system comprises a single entity (Bolosky: Fig. 3).

Claim Rejections - 35 USC § 103

6. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

(a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negated by the manner in which the invention was made.

7. Claims 3 and 36 are rejected under 35 U.S.C. 103(a) as being unpatentable over Bolosky et al. (7,043,637) in view of Schneier (Applied Cryptography).

a) As to claim 3, Bolosky discloses a method as claimed in claim 1, however it is silent on the capability of the first set of data is encrypted by performing an exclusive OR operation between the first set of data and the second set of data. Schneier is relied on for the teaching of the first set of data is encrypted by performing an exclusive OR operation between the first set of data and the second set of data (i.e. the plaintext is being XORed with a keyword to generate the ciphertext, Schneier: page 14). It would have been obvious to one of ordinary skill in the art at the time of the invention to employ the use of the first set of data is encrypted by performing an exclusive OR operation between the first set of data and the second set of data in the system of Bolosky, as Schneier teaches, so as to provide another way of encrypting data.

b) As to claim 36, this claim is directed to a system implementation of the method of claim 3, therefore it is rejected by a similar rationale applied against claim 3 above.

Art Unit: 2137

8. Claims 6-7, 9-11, 16, 18-19, 21-24, 26, 29-30, 37-38, 40 and 46 are rejected under 35 U.S.C. 103(a) as being unpatentable over Bolosky et al. (7,043,637) in view of Suzuki et al. (6,704,119).

a) As to claim 6, Bolosky discloses the method of claim 1, however it is silent on the capability of having an encrypted first set of data is stored at a first node. Suzuki is relied on for the teaching of having an encrypted first set of data (i.e. first set of data is generated by multi-function peripheral (MFP) (see Suzuki: Fig. 1, element 11; col. 4, lines 59-61; col. 5, lines 27-28) is stored at a first node (e.g. server, see Suzuki: col. 6, lines 48-50; col. 12, lines 36-39). It would have been obvious to one of ordinary skill in the art at the time of the invention to employ the use of having an encrypted first set of data is stored at a first node in the system of Bolosky, as Suzuki teaches, so as to store and archive file data (Suzuki: col. 1, lines 15-22).

b) As to claim 7, the combination of Bolosky and Suzuki discloses the method of claim 6, further comprising the step of storing the second set of data in a memory of a second node (i.e. storing in a computer, Bolosky: Fig. 2, element 226).

c) As to claim 9, the combination of Bolosky and Suzuki discloses the method of claim 6, further comprising the steps of transmitting the encrypted first set of data from the second node (e.g. MFP) to the first node (e.g. server, Suzuki: col. 12, lines 36-39).

d) As to claim 10, the combination of Bolosky and Suzuki discloses the method of claim 6, further comprising the step of storing the encrypted first set of data at a location on said first node (Suzuki: col. 9, lines 1-5).

e) As to claim 11, the combination of Bolosky and Suzuki discloses the method of claim 6, further comprising the step of transmitting address information of a location at which the first set of data is stored from the first node to said second node (i.e. location specified in additional data is supplied in the transmission instruction indicates location address is provided and now being used to access data in the server, Suzuki, col. 6, lines 23-30).

f) As to claim 16, the combination of Bolosky and Suzuki discloses the method of claim 6, further comprising the step of decrypting the encrypted first set of data using the second set of data (i.e. using the second set of data as a symmetric key, therefore the same key is used for both encryption and decryption, Bolosky: col. 5, lines 42-44).

g) As to claim 18, the combination of Bolosky and Suzuki discloses the method of claim 6, further comprising transmitting a request to download the encrypted first set of data to the address of a location at which the encrypted first set of data is stored (i.e. document data is encrypted in the image processing unit of MFP 11, then is transmitted and stored in server 12, Suzuki: col. 12. lines 36-39; encrypted document data is transmitted to MFP 11, Suzuki: col. 6, lines 48-50) and decrypting the encrypted first set of data (i.e. encrypting/decrypting process using the same key, Bolosky: col. 5, lines 42-43)

h) As to claim 19, the combination of Bolosky and Suzuki discloses the method of claim 6, further comprising and downloading the encrypted first set of data from the first node to the second node (encrypted document data is transmitted to MFP

11, Suzuki: col. 6, lines 48-50) and decrypting the encrypted first set of data (i.e. encrypting/decrypting process using the same key, Bolosky: col. 5, lines 42-43).

i) As to claim 21, the combination of Bolosky and Suzuki discloses the method of claim 6, wherein the second set of data is generated at a second node (i.e. checksum is generated in a computer, Bolosky: Fig. 2, element 226).

j) As to claim 22, the combination of Bolosky and Suzuki discloses the method of claim 6, wherein the first set of data is encrypted at the second node (i.e. the software program is encrypted in a computer, Bolosky: Fig. 2, element 224).

k) As to claim 23, the combination of Bolosky and Suzuki discloses the method of claim 6, wherein the first node comprises a first network archive server (e.g. server 12, Suzuki: col. 6, lines 31-40, lines 48-57).

l) As to claim 24, the combination of Bolosky and Suzuki discloses the method of claim 7, wherein the second node comprises a piece of user equipment (i.e. computer, Bolosky: Fig. 1, element 108).

m) As to claim 26, the combination of Bolosky and Suzuki discloses the method of claim 24, wherein the user equipment comprises one of a mobile station, a digital camera, a personal digital assistant or a personal computer (i.e. computer, Fronberg: Fig. 1, element 108).

n) As to claim 29, the combination of Bolosky and Suzuki discloses the method of claim 7, further comprising creating the first set of data by the second node (i.e. data file, Bolosky: col. 4, lines 36-38).

o) As to claim 30, the combination of Bolosky and Suzuki discloses the method of claim 7, further comprising receiving the first set of data at the second node from a third party (e.g. PC 14, Suzuki: col. 6, lines 6-8).

p) As to claim 37, this claim is directed to a system implementation of the method of claim 6, therefore it is rejected by a similar rationale applied against claim 6 above.

q) As to claim 38, the combination of Bolosky and Schneier discloses the method of claim 37, further comprising a second node comprising storage means configured to store the second set of data (i.e. storing in a computer, Bolosky: Fig. 2, element 220).

r) As to claim 40, the combination of Bolosky and Schneier discloses the method of claim 38, wherein the second node further comprises the encrypting means (Bolosky: Fig. 2, element 224).

s) As to claim 46, the combination of Bolosky and Suzuki discloses the system of claim 38, wherein the second node comprises a piece of user equipment (i.e. computer, Bolosky: Fig. 1, element 108).

9. Claims 8, 12-15, 20, 25, 39 and 52 are rejected under 35 U.S.C. 103(a) as being unpatentable over Bolosky et al. (7,043,637) in view of Suzuki et al. (6,704,119) and further in view of Marvit et al. (6,625,734).

a) As to claim 8, the combination of Bolosky and Suzuki discloses the method of claim 7, however it is silent of the capability of storing the second set of data

at a third node. Marvit is relied on for the teaching of storing the second set of data (e.g. unique key associated with message ID) at a third node (e.g. key repository) (i.e. storing key in the key repository, Marvit: col. 4, lines 41-43). It would have been obvious to one of ordinary skill in the art at the time of the invention to employ the use of storing the second set of data at a third node in the system of Bolosky and Suzuki, as Marvit teaches, so as to securely and effectively control and track access to data (Marvit: col. 3, lines 60-61).

b) As to claim 12, the combination of Bolosky and Suzuki discloses the method of claim 11, however it is silent on the capability of the transmitting the address information comprises transmitting a uniform resource locator. Marvit is relied on for the teaching of the transmitting the address information comprises transmitting a uniform resource locator (i.e. the recipient is provided with a message's URL that specifies the location of the message, Marvit: col. 19, lines 55-59). It would have been obvious to one of ordinary skill in the art at the time of the invention to employ the use of the transmitting the address information comprises transmitting a uniform resource locator in the system of Bolosky and Suzuki, as Marvit teaches, so as to control and track access to data on communication network (Marvit: col. 2, lines 1-5).

c) As to claim 13, the combination of Bolosky, Suzuki and Marvit discloses the method of claim 8, further comprising the step of storing the second set of data at a location on said third node (i.e. storing the second set of data at a specific location on the key repository, Marvit: Fig. 2, element 204).

d) As to claim 14, the combination of Bolosky, Suzuki and Marvit discloses the method of claim 13, further comprising the step of transmitting address information of the location at which the second set of data is stored from said third node to said second node (i.e. the combination of Bolosky and Suzuki teaches transmitting address information of a location at which the first set of data is stored from the first node to said second node (i.e. location specified in additional data is supplied in the transmission instruction indicates location address is provided and now being used to access data in the server, Suzuki, col. 6, lines 23-30), this concept can be implemented for transmitting address information of the location at which the second set of data is stored from said third node to said second node as it is done with the first set of data).

e) As to claim 15, the combination of Bolosky, Suzuki and Marvit discloses the method of claim 14, wherein the transmitting the address information comprises transmitting a uniform resource locator. Marvit teaches the transmitting the address information comprises transmitting a uniform resource locator (i.e. the recipient is provided with a message's URL that specifies the location of the message, Marvit: col. 19, lines 55-59, this concept can be implemented to provide the address information at which the second set of data is stored is a URL as it is done with the first set of data).

f) As to claim 20, the combination of Bolosky and Suzuki discloses the method of claim 19, further comprising decrypting the encrypted first set of data (i.e. encrypting/decrypting process using the same key, Bolosky: col. 5, lines 42-44), however it is silent on the capability of downloading the second set of data from the third node to the second node. Marvit is relied on for the teaching of downloading the second

Art Unit: 2137

set of data from the third node to the second node (i.e. downloading key from key repository, Marvit: col. 3, lines 52-55). It would have been obvious to one of ordinary skill in the art at the time of the invention to employ the use of downloading the second set of data from the third node to the second node in the system of Bolosky and Suzuki, as Marvit teaches, so as to be able to access to the protected data (Marvit: col. 3, lines 48-50).

g) As to claim 25, the combination of Bolosky, Suzuki and Marvit discloses the method of claim 8, wherein the storing at the third node comprises storing at a second network archive server (e.g. key repository, Marvit: Fig. 2, element 106).

h) As to claim 39, this claim is directed to a system implementation of the method of claim 8, therefore it is rejected by a similar rationale applied against claim 8 above.

i) As to claim 52, the combination of Bolosky and Suzuki discloses the system of claim 37, however it is silent on the capability of having a deletion unit configured to delete the encrypted first set of data from the first node after the encrypted first set of data has been downloaded. Marvit is relied on for the teaching of having a deletion unit configured to delete the encrypted first set of data from the first node after the encrypted first set of data has been downloaded (i.e. deletion message from specified location after message has been retrieved from the specified location, Marvit: col. 18, lines 42-45). It would have been obvious to one of ordinary skill in the art at the time of the invention to employ the use of having a deletion unit configured to delete the encrypted first set of data from the first node after the encrypted first set of data has

been downloaded in the system of Bolosky and Suzuki, as Marvit teaches, so as to control storing and archiving processed data.

10. Claim 17 is rejected under 35 U.S.C. 103(a) as being unpatentable over Bolosky et al. (7,043,637) in view of Suzuki et al. (6,704,119) and further in view of Schneier ((Applied Cryptography).

The combination of Bolosky and Suzuki discloses the method of claim 6, however it is silent on the capability of decrypting the encrypted first set of data by performing an exclusive OR operation between the encrypted first set of data and the second set of data. Schneier is relied on for the teaching of decrypting the encrypted first set of data by performing an exclusive OR operation between the encrypted first set of data and the second set of data (i.e. the ciphertext is being XORed with a keyword to generate the plaintext, Schneier: page 14). It would have been obvious to one of ordinary skill in the art at the time of the invention to employ the use of the first set of data is encrypted by performing an exclusive OR operation between the first set of data and the second set of data in the system of Bolosky and Suzuki, as Schneier teaches, so as to provide another way of decrypting data.

11. Claims 28 and 50 are rejected under 35 U.S.C. 103(a) as being unpatentable over Bolosky et al. (7,043,637) in view of Bloomberg (5,765,176).

a) As to claim 28, Bolosky discloses the method of claim 1, however he is silent on the capability of having the generating the second set of data comprises

Art Unit: 2137

generating one of a thumbnail image, an extract from an audio file or a picture of a multimedia message. Bloomberg is relied on for the teaching of the second set of data comprises one of a thumbnail image, an extract from an audio file or a picture of a multimedia message (i.e. an icon image or thumbnail image represents larger document, Bloomberg: col. 1, lines 28-51). It would have been obvious to one of ordinary skill in the art at the time of the invention to employ the use of having the generating the second set of data comprises generating one of a thumbnail image, an extract from an audio file or a picture of a multimedia message in the system of Bolosky, as Bloomberg teaches, so as to perform document image management tasks related to the text image (Bloomberg: col. 1, lines 25-27).

b) As to claim 50, this claim is directed to a system implementation of the method of claim 28, therefore it is rejected by a similar rationale applied against claim 28 above.

12. Claim 31 is rejected under 35 U.S.C. 103(a) as being unpatentable over Bolosky et al. (7,043,637) in view of Suzuki et al. (6,704,119) and further in view of Wang et al (6,173,406).

The combination of Bolosky and Suzuki discloses the method of claim 7, however it is silent on the capability of sending address information of a location at which the encrypted first set of data is stored, and the second set of data to a third party. Wang is relied on for the teaching of sending the address information of a location at which the encrypted first set of data is stored, and the second set of data (e.g.

password) are sent to a third party (e.g. video server) (i.e. user provides specified URL, where URL links to a selected multimedia content, and password to the video server, Wang: col. 5, lines 20-65). It would have been obvious to one of ordinary skill in the art at the time of the invention to employ the use of sending the address information of a location at which the encrypted first set of data is stored, and the second set of data to a third party in the system of Bolosky and Suzuki, as Wang teaches so as to control content presentation and reproduction by unauthorized and unauthenticated users of media content distributed over networks (Wang: col. 1, lines 35-38).

13. Claim 32-33 are rejected under 35 U.S.C. 103(a) as being unpatentable over Bolosky et al. (7,043,637) in view of Suzuki et al. (6,704,119) and further in view of Sull et al. (2002/0069218).

a) As to claim 32, the combination of Bolosky and Suzuki discloses the method of claim 11, however it is silent on the capability of storing the address information of the location at which the encrypted first set of data is stored, in the second set of data as a watermark. Sull is relied on for the teaching of storing the address information of the location at which the encrypted first set of data is stored, in the second set of data as a watermark (i.e. URL can be encoded into a thumbnail image and the image encoded with the texts can be used in watermarking technology, Sull: paragraph 0265). It would have been obvious to one of ordinary skill in the art at the time of the invention to employ the use of having the address information of the location at which the encrypted first set of data is stored, is stored in the second set of data as a

watermark in the system of Bolosky and Suzuki, as Sull teaches so as to facilitate storing, searching and retrieving the multimedia information (Sull: paragraph 0002).

b) As to claim 33, the combination of Bolosky and Suzuki discloses the method of claim 11, however it is silent on the capability of the transmitting the address information comprises transmitting address information derivable from the second set of data. Sull is relied on for the teaching of the transmitting the address information comprises transmitting address information derivable from the second set of data (i.e. URL of a video file can be encoded into a thumbnail image, therefore URL can be derivable from the thumbnail image, Sull: paragraph 0265)). It would have been obvious to one of ordinary skill in the art at the time of the invention to employ the use of the transmitting the address information comprises transmitting address information derivable from the second set of data in the system of Bolosky and Suzuki, as Sull teaches, so as to retrieve multimedia data using its location identification data encoded in thumbnail image.

14. Claims 41-42, 44-45 and 47 are rejected under 35 U.S.C. 103(a) as being unpatentable over Bolosky et al. (7,043,637) in view of Schneier (Applied Cryptography) and in view of Suzuki et al. (6,704,119).

a) As to claim 41, the combination of Bolosky and Schneier discloses the system of claim 38, however it is silent on the capability of having the second node further comprises a transmitting unit configured to transmit the encrypted first set of data to the first node. Suzuki is relied on for the teaching of having the second node (e.g.

Art Unit: 2137

MFP) further comprises a transmitting unit configured to transmit the encrypted first set of data to the first node (e.g. server) (see Suzuki: col. 12, lines 36-39). It would have been obvious to one of ordinary skill in the art at the time of the invention to employ the use of having the second node further comprises a transmitting unit configured to transmit the encrypted first set of data to the first node in the system of Bolosky and Schneier, as Suzuki teaches, so as to store and archive file data (Suzuki: col. 1, lines 15-22).

b) As to claim 42, the combination of Bolosky and Schneier discloses the system of claim 38, however it is silent on the capability of having the second node further comprises a capturing unit to capture the first set of data. Suzuki is relied on for the teaching of having the second node (e.g. MFP) further comprises a capturing means to capture the first set of data (i.e. MFP 11 can be used as a copy machine, a facsimile machine, a printer and a scanner, any of those devices can capture the first set of data, see Suzuki: col. 5, lines 27-28). It would have been obvious to one of ordinary skill in the art at the time of the invention to employ the use of having the second node further comprises a capturing unit to capture the first set of data in the system of Bolosky and Schneier, as Suzuki teaches, so as to collect and process captured data (Suzuki: col. 1, lines 15-22).

c) As to claim 44, the combination of Bolosky, Schneier and Suzuki discloses the system of claim 43, wherein the decrypting unit is configured to decrypt the encrypted first set of data by performing an exclusive OR operation between the

encrypted first set of data and the second set of data (i.e. the ciphertext is being XORed with a keyword to generate the plaintext, Schneier: page 14).

d) As to claim 45, the combination of Bolosky and Schneier discloses the system of claim 37, however it is silent on having the first node comprises a first network archive server. Suzuki is relied on for the teaching of having the first node comprises a first network archive server (e.g. server 12, Suzuki: col. 6, lines 31-40, lines 48-57). It would have been obvious to one of ordinary skill in the art at the time of the invention to employ the use of having the first node comprises a first network archive server in the system of Bolosky and Schneier, as Suzuki teaches, so as to store and archive file data (see Suzuki: col. 1, lines 15-22).

e) As to claim 47, the combination of Bolosky, Schneier and Suzuki discloses the system of claim 46, wherein the user equipment comprises one of a mobile station, a digital camera, a personal digital assistant or a personal computer (i.e. computer, Bolosky: Fig. 1, element 112).

15. Claim 48 is rejected under 35 U.S.C. 103(a) as being unpatentable over Bolosky et al. (7,043,637) in view of Schneier (Applied Cryptography) and further in view of Marvit (6,625,734).

The combination of Bolosky and Schneier discloses the system of claim 39, however it is silent on the capability of having the third node comprises a second network server archive. Marvit is relied on for the teaching of having the third node comprises a second network server archive (e.g. key repository, Marvit: Fig. 2, element

Art Unit: 2137

106). It would have been obvious to one of ordinary skill in the art at the time of the invention to employ the use of having the third node comprises a second network server archive in the system of Bolosky and Schneier, as Marvit teaches so as to store and archive processed data.

16. Claims 53-54 are rejected under 35 U.S.C. 103(a) as being unpatentable over Bolosky et al. (7,043,637) in view of Marvit (6,625,734).

b) As to claim 53, Bolosky discloses the system of claim 34, however it is silent on the capability of having a node for storing the encrypted first set of data. Marvit is relied on for the teaching of having a node for storing the encrypted first set of data (i.e. message repository for storing the encrypted message, Marvit: col. 18, lines 46-60). It would have been obvious to one of ordinary skill in the art at the time of the invention to employ the use of having a node for storing the encrypted first set of data in the system of Bolosky, as Marvit teaches so as to provide a means for storing and archiving processed data.

c) As to claim 54, the combination of Bolosky and Marvit discloses the system of claim 53, wherein said node is a network archive server (e.g. message repository, Marvit: Fig. 9, element 906).

Conclusion

17. Applicant's amendment necessitated the new ground(s) of rejection presented in this Office action. Accordingly, **THIS ACTION IS MADE FINAL**. See MPEP

§ 706.07(a). Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).


A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the date of this final action.

18. Any inquiry concerning this communication or earlier communications from the examiner should be directed to Minh Dieu Nguyen whose telephone number is 571-272-3873.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Emmanuel Moise can be reached on 571-272-3865. The fax phone number for the organization where this application or proceeding is assigned is (571) 273-8300.

Art Unit: 2137

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see <http://pair-direct.uspto.gov>. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).


mdn
8/13/07


EMMANUEL L. MOISE
SUPERVISORY PATENT EXAMINER